United Nations S/2004/132

Security Council

Distr.: General
20 February 2004

Original: English

Letter dated 17 February 2004 from the Chairman of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism addressed to the President of the Security Council

I write with reference to my letter of 21 November 2003 (S/2003/1122). The Counter-Terrorism Committee has received the attached fourth report from Canada submitted pursuant to paragraph 6 of resolution 1373 (2001) (see annex). I would be grateful if you could arrange for the present letter and its annex to be circulated as a document of the Security Council.

(*Signed*) Inocencio F. **Arias**
Chairman
Security Council Committee established pursuant to
resolution 1373 (2001) concerning counter-terrorism

04-24787 (E) 230304

Annex

Note verbale dated 12 February 2004 from the Permanent Mission of Canada to the United Nations addressed to the Chairman of the Counter-Terrorism Committee

The Permanent Mission of Canada to the United Nations presents its compliments to the Chairman of the Committee, and has the honour to forward Canada's fourth report regarding the implementation of resolution 1373 (2001) (see enclosure).

Enclosure

Implementation of United Nations Security Council Resolution 1373
Canada's Fourth Report to the United Nations Counter-Terrorism Committee

1.1 The CTC would appreciate learning whether the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) has sufficient resources (human, financial and technical) to enable it to carry out its mandate.

The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) is a specialized agency created to receive, analyze, assess and disclose financial intelligence on suspected money laundering and terrorist activity financing. The Centre became operational in October 2001, and the final reporting obligations were implemented in March 2003. FINTRAC is an integral part of the Government of Canada's commitment to the fight against money laundering and terrorist financing.

Under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA), FINTRAC provides law enforcement and intelligence agencies with financial intelligence on suspected money laundering, terrorist activity financing and threats to the security of Canada. In addition, the Centre may also provide information to foreign Financial Intelligence Units (FIUs) provided it has entered into an agreement governing such an exchange. FINTRAC has an annual budget of $32M (CAD), and a staff complement of 194 (as of December 2003). As noted in the recent Three-Year Evaluation of the National Initiative to Combat Money Laundering, FINTRAC is operational and is making disclosures to the appropriate law enforcement agencies. The Centre continues to enhance its technical capacity, and will continue to improve its technical means to sift through the more than 9 million reports it receives each year. FINTRAC is meeting its current obligations, but may require additional resources in future as it strives to optimize its analytical capacity and meet new challenges presented by a changing criminal and technological landscape.

1.2 Could Canada please indicate how many money remittance/transfer services are registered and/or licensed in Canada? Please outline the legal provisions that it has put in place to prevent informal money/value transfer systems from being used for the purpose of financing terrorism. In the absence of such provisions, could Canada indicate the steps that it intends taking in order to fully comply with this aspect of the Resolution.

Money services businesses (MSBs), including alternative remittance systems, are subject to the PCMLTFA. As other financial institutions and intermediaries, they are required to ascertain the identity of their clients, maintain records of certain transactions and file suspicious and prescribed financial transaction reports with Canada's financial intelligence unit, FINTRAC.

Currently, there are no registration or licensing requirements in Canada for money remitters. Canada is currently looking at options to establish a registration system for MSBs.

1.3 Would Canada please provide the CTC with the number of suspicious transaction reports (STR) received by FINTRAC and other competent authorities?

Financial institutions and intermediaries that are designated as reporting entities under the PCMLTFA must submit a Suspicious Transaction Report (STR) for any financial transactions that occur where there are reasonable grounds to suspect they are related to the commission of a money laundering offence or a terrorist activity financing offence.

For the fiscal year 2002/2003, FINTRAC was receiving a monthly average of 1,433 STRs. This was an increase over the previous year's average of 744 STRs per month. It should be noted however that the requirement to report STRs only came into effect in November 2001. Between November 2001 and March 2003, FINTRAC received a total of 17,197 STRs. Reporting by sector is as follows:

- 55% Financial Entities (Banks, Credit Unions, Caisses populaires, Trust and Loan companies)
- 40% Foreign Exchange Dealers and Money Services Businesses
- 5% Others (Casinos, Life Insurance, Real Estate, Securities Dealers and others)

Suspicious Transaction Reports are important to our analysis, and have figured in a significant number of our disclosures.

1.4 The CTC would be grateful if Canada could outline its principal legal procedures concerning the confiscation of assets or the operation of other deprivation mechanisms.

Constitutional competence - Canada is a federation, in which the federal Parliament has exclusive constitutional competence to enact legislation in relation to the criminal law, which includes procedural and substantive laws relating to the prevention and suppression of terrorism. The administration of criminal justice, including law-enforcement and prosecution is generally a matter for the provinces, but substantial federal jurisdiction has been established to deal with a number of federal offences and criminal justice matters of an inter-provincial or international nature. In the case of the *Criminal Code* anti-terrorism provisions, the statute provides that either the federal or a provincial Attorney-General may prosecute, allowing decisions to be made on a case-by-case basis. Federal law-enforcement and security authorities would generally have the lead on terrorism cases, with provincially-established police forces, including municipal forces, involved as necessary depending on the facts of each case. In exercising statutory powers addressed to "any peace officer", within a province, any federal officer or any officer designated as such by that province, may so act.

Freezing of property - In terrorist asset cases (i.e. any property that is owned or controlled by or on behalf of a terrorist group), freezing occurs automatically by operation of the statute, without the need for any decision or action on the part of executive or judicial authorities. The relevant provision applies in any case where any person in Canada or any Canadian outside Canada knows they possess, deal with, directly or indirectly such property, or undertake transactions, financial or related services in respect of such property. Canadian law also allows the criminalisation of cases where the accused was "wilfully blind" (intentionally ignorant) as to essential facts in some circumstances, and the

freezing prohibitions extend to cases where, in the face of some basis to believe the property might be owned or controlled by or on behalf of a terrorist group, the person dealing in them remained deliberately ignorant of its nature. Since no judicial or executive decision or authority is involved, the freezing occurs without any acts of seizure or restraint. The statutory freeze operates directly as a prohibition on any dealings, transactions or services in respect of such property and would apply to anyone in possession of the property or otherwise in a position to do any of the prohibited activities. Breaches of the freezing obligations are subject to prosecution as a criminal offence under a separate provision, punishable by up to 10 years' imprisonment.

Reporting or disclosure of property or transactions - In any case where a person knows that property in their possession or control is owned by or controlled by or on behalf of a terrorist group or has information about any transaction or proposed transaction in respect of such property, there is a positive obligation to immediately disclose the existence of the asset or information about the transaction to the Commissioner of the Royal Canadian Mounted Police (RCMP) and the Director of the Canadian Security Intelligence Service (CSIS). There is also a further requirement to report the same information to FINTRAC. Information reported to the RCMP Commissioner can, where appropriate, be transmitted to any other law-enforcement agency in Canada. FINTRAC can use the report as part of its bank of information to further assess criminal money-laundering and terrorist financing activity. In addition to any follow-up investigations by law-enforcement or CSIS, prosecutors can be asked to seek authority to seize or assume management control over the property. The Commissioner of the RCMP, and the Directors of FINTRAC and CSIS are all senior federal appointees, subject to the statutory mandates and oversight structures of their respective organisations.

Seizure or restraint of property - A statutory freeze under s.83.08 prohibits any dealings in the property but does not affect possession or management, for which seizure or restraint is required. Several options are available for this under Canadian law. Generally, forms of judicial search-warrant can be obtained to search for and seize property which is evidence, proceeds of a crime or "offence-related property". These usually involve physical seizure and are used for moveable and tangible property. Judicial restraint orders can also be obtained. These prohibit any disposal or other dealing in the specified property and are generally used for property that is immoveable (land etc.) or intangible (bank accounts etc.). They may be sought from a court by the relevant federal or provincial official (procedures vary). Search warrants are executed by the appropriate peace officers, whereas restraining orders operate directly on those in possession or control of the specified property. All may be obtained *ex parte* and are subject to later judicial review and opportunities for those affected to challenge the basis of the order or the manner in which it was executed. All of these categories of property are linked to the terrorism offences, so that property that is related in some way to terrorist activities, or in the case of proceeds, property that is the proceeds of a terrorist offence, will be subject to seizure or restraint under the appropriate provision.

(a) In the case of moveable property that may be criminal evidence a criminal search warrant can be obtained from a judicial officer, authorizing the physical seizure of the property.

(b) In the case of property which is "offence-related property" (property used in or intended for use in a serious crime, or by means of which a serious crime is committed) a judicial officer may issue

a warrant to search for and seize property specified in the warrant. Such warrants may be executed by any peace officer or any specific person named in the warrant. They may be used to seize moveable property that is in Canada, or as the basis of a mutual legal assistance request that a foreign State seize moveable property that is outside of Canada. Restraint orders (below) are used for immoveable or intangible property and may also be used for property outside of Canada, to the extent that persons within the jurisdiction of the issuing court can be ordered not to deal in such property. Restraint orders must be served on those bound by them, and in the case of persons outside the jurisdiction of the court reciprocal enforcement may be requested of other States.

(c) If the property is moveable property and is the proceeds of a crime, including any terrorist offence, the relevant Attorney General can seek a special search warrant to search for and seize the property. "Proceeds of crime" is defined broadly, including "any property, benefit or advantage, within or outside Canada, obtained or derived directly or indirectly as a result of the commission in Canada of a designated offence, or an act or omission anywhere that, if it had occurred in Canada, would have constituted a designated offence". The term "designated offence" encompasses all major criminal offences, including terrorism-related offences, and in particular the financing offences which implement the *International Convention for the Suppression of the Financing of Terrorism, 1999*, as well as the other offences which could be used to generate proceeds to finance terrorism, such as fraud, kidnapping or robbery. Such warrants may be executed by any peace officer or any specific person named in the warrant, and are subject to later review by the courts. They are generally used as a first step toward seeking the forfeiture of the proceeds.

(d) Judicial restraining orders are usually used in cases where the property cannot be physically seized using a warrant. These orders prohibit any person from disposing of or otherwise dealing with any interest in the specified property. An order sought under *Criminal Code* s.462.33 may be obtained in respect of "any property". An order may also be sought under *Criminal Code* s.490.8 in respect of any "offence-related property". This is the Canadian term that refers to instrumentalities, and includes property used or destined for use in a serious crime or "by means of or in respect of" such a crime is committed. The category of crimes to which the definition is linked includes all of the terrorism offences, which means that both types of restraining order are available in such cases. Restraining orders are available for any form of property, but are most commonly used for those forms that are not amenable to physical seizure, such as immovable (land etc.) and intangible (bank accounts etc.) property. These orders are issued by a court on the application of a prosecutor and are subject to subsequent review by the courts. They are served on the natural or legal person to whom they are addressed (e.g., banks and similar institutions), and where applicable to land are included in official records that must be checked prior to any transfer, such as land title registries.

(e) Through amendments to the *Criminal Code,* the *Anti-terrorism Act* created an additional power to restrain property linked to terrorist groups. Where there are reasonable grounds to believe that property is owned or controlled by or on behalf of a terrorist group or that it has been or will be used, in whole or in part, to facilitate or carry out a terrorist activity, its seizure or restraint and forfeiture may be sought (regarding seizure, see subparagraph (b), above). In such cases, based on information from law enforcement or CSIS, counsel for the Attorney General would seek orders for seizure or restraint from a Judge of the Federal Court of Canada. A warrant could be issued to search

for and seize any property located in Canada. A restraining order prohibiting anyone in the jurisdiction of the court from dealing in the property could be issued in respect if any property, and would generally be issued in respect of any property outside of Canada, and for any property in Canada not amenable to physical seizure, such as immovable property (e.g., land) and intangible property (e.g., bank accounts). The legislation provides for use of these powers by either federal or provincial law enforcement officials and Attorneys-General, and either may apply for the orders before the Federal Court. In most terrorism-related cases, however, these would be used by the appropriate federal agencies and officials because of the international and inter-provincial nature of the cases.

Seizure or restraint in transnational cases - The various seizure and restraint orders are available in response to mutual legal assistance requests under the *Convention for the Suppression of the Financing of Terrorism*, as well as other criminal law treaties containing mutual legal assistance provisions. Orders for the gathering of evidence, which require a third party to produce records or provide testimony, may also be useful in some cases. Evidence can be obtained, assets that were instrumentalities (for Canadian purposes, "offence related property") and proceeds of crime may be seized and restrained. These requests are implemented under Canada's *Mutual Legal Assistance in Criminal Matters Act*. Requests are submitted through the usual mutual assistance channels; approved by the Minister of Justice's International Assistance Group and assigned to counsel for the Attorney General of Canada or a Province to obtain the essential court orders or file the required documents with a superior court of criminal jurisdiction in Canada. Canadian law enforcement agencies enforce such orders, including the conduct of any search or seizure required, and the serving of restraint or attendance orders on those identified or likely to be affected by them within Canada.

Management of seized or restrained property - To protect legitimate interests and minimise any economic losses, Canadian law provides powers to manage property that has been seized or restrained, pending any final disposition of such property. The provisions apply equally to property seized or restrained as a result of domestic applications and applications made pursuant to mutual legal assistance requests. The provisions allow the court that orders seizure or restraint to impose terms and conditions. The authority to manage includes the authority to sell, in the case of property that is rapidly depreciating or perishable. Subject to court approval, on notice to persons with a valid interest, property that is of little or no value may be destroyed. On the request of the Attorney General of Canada, the court may appoint the Minister of Public Works and Government Services as manager, and in this case the property is managed by a professional property management section of that ministry under the authority of the *Seized Property Management Act*. Other provision is made for management when the request originates with the Attorney General of a province, but this will not usually arise in terrorist-financing cases.

Relief from seizure or restraint - As noted, seizure and restraint orders are initially obtained on an *ex parte* basis, but are open to subsequent judicial review. There is a continuing right to seek relief from these orders, from the time the order is issued or executed. Any person who has a valid interest in the property may apply to a court for relief, with notification to counsel for the (federal or provincial) Attorney General on whose application the original order was issued. Forms of relief include a right to seek access to the relevant property to fund reasonable legal, living and business expenses. The

court must consider the applicant's other assets and the appropriate legal aid tariff (rates). The right to seek relief ends if any forfeiture order is issued against the property. Relief is normally sought in a court of criminal jurisdiction, but may also be sought in the Federal Court of Canada in some cases.

Forfeiture - As noted, the powers of seizure and restraint, other than those to seize property as evidence in criminal cases, generally conclude with proceedings to forfeit (confiscate) the property, in a court of criminal jurisdiction. In the case of property owned or controlled by or on behalf of a terrorist group and property that has been or will be used, in whole or in part, to facilitate or carry out a terrorist activity, criminal forfeiture may still apply where appropriate, and forfeiture may also be sought though a civil application in the Federal Court of Canada. A final foreign criminal forfeiture order can also be enforced in Canada. In such cases, a request is submitted through the usual mutual assistance channels, approved by the Minister of Justice's International Assistance Group, and assigned to counsel for the Attorney General of Canada or a Province. Counsel then seeks enforcement by superior court of criminal jurisdiction in Canada. When a criminal court or the Federal Court orders forfeiture or the enforcement of a foreign order any seizure or other enforcement measures are taken by the appropriate law enforcement agency.

Steps taken after forfeiture - All forfeited assets are forfeited to the State, which may be the federal or a provincial government, depending upon the specific forfeiture application and the Attorney General who instituted it. Forfeiture orders are final, subject to periods for appeal set out in the statutory provisions. The status of the applicant Attorney General is important since all forfeiture provisions specify that the property is forfeited "to be disposed on as the Attorney General directs or otherwise dealt with in accordance with law". This means that the forfeited property is generally forfeited to either the federal or a provincial Attorney General, depending on which level of government initiated the proceedings. In forfeitures to the Attorney General of Canada the *Seized Property Management Act* applies and controls the forfeited property. Forfeiture could occur on any of the following authorities:

(a) The asset is offence related property (*Criminal Code*, s. 490.1);

(b) The asset is proceeds of crime (*Criminal Code*, sections 462.38 or 462.78);

(c) The seized asset's owner is unknown or the person from whom it was seized or restrained was unlawfully in possession. (*Criminal Code* sections 462.38 or 462.78);

(d) The asset is forfeited by the Federal Court of Canada as terrorism-related property (*Criminal Code*, section 83.14). Two alternatives exist for those specific forfeitures.

(i) They may be treated exactly like any other forfeiture, with the forfeited property passing to the relevant federal or provincial government, depending upon which Attorney General instituted the successful forfeiture application (section 83.14 paragraph (5)); or

(ii) Regulations may provide that the forfeiture is used to compensate victims of terrorist activities and to fund anti-terrorist initiatives. (Section 83.14, paragraphs (5.1)-(5.2)].

It is possible to confiscate the proceeds without first obtaining the conviction of the perpetrator (i.e. *in rem* confiscation). Canada's established regime for dealing with the forfeiture of proceeds of crime

has provided for forfeiture in cases where there is no criminal conviction, since 1988. Under the present law both proceeds of crime and offence-related property can be forfeited in the absence of a criminal conviction where it is proved beyond a reasonable doubt that the property is proceeds or offence-related property, and that legal proceedings have been started in respect of the related offence, but the person who would have been prosecuted has died or absconded. These provisions could be applied in cases where the property was proceeds of a terrorist offence or related to such an offence. The 2001 amendments have also added specific powers to forfeit property that is owned or controlled by or on behalf of a terrorist group, and property that has been or will be used to facilitate or carry out any terrorist activity. These provide a more general forfeiture authority: provided that the necessary link to a terrorist group or terrorist activity is established, there is no requirement that any individual terrorist offender or perpetrator be identified, prosecuted or convicted.

This provision can also be used in respect of property seized for any reason, whether this was done as a terrorist asset, as offence-related property, criminal evidence, proceeds of crime or for any other reason, or against property that has not been seized or restrained. This could occur, for example, in cases where the property is caught by a statutory freeze. The identification of the property and its link to terrorist groups or activities need only be proven on a balance of probabilities, a lower standard than the Canadian criminal law requirement of proof beyond a reasonable doubt. Forfeiture orders in respect of terrorist assets may be obtained only from the Federal Court of Canada, on the application of either the federal or a provincial Attorney General, and where forfeiture is ordered, the property can be disposed of as the Attorney General which sought the forfeiture directs.

There are appellate provisions allowing for review of the decisions taken by the authorities. All proceedings which result in powers of search, seizure, and restraint of property of any kind in Canada may be initiated *ex parte*, but are subject to some form of appeal or judicial review or scrutiny after the action is taken, with appropriate remedies where it is found to have exceeded the authority granted or where the underlying basis of the action is subsequently found to be deficient in some way. In addition to substantive and procedural grounds under the relevant legislation, such activities are also held to a basic constitutional standard that guarantees the right to be free of unreasonable search or seizure and subject to possible remedies that include the exclusion of evidence.

The specific mechanisms for such reviews and remedies vary according to the nature of the action authorized, the property in respect of which it was taken, and other factors, and details are set out in the previous responses for each power. Generally, reviews and appeals of powers used in criminal cases are heard by courts of criminal jurisdiction, often as a preliminary matter preceding a related criminal prosecution, or as an issue on the appeal of a criminal conviction. The provisions specifically governing the seizure, restraint and forfeiture of terrorism-related property, *Criminal Code* sections 83.13 and 83.14 are not dealt with by ordinary criminal courts and do not set out a specific appeal process. Since the forfeiture proceedings are not *ex parte*, notice is given to persons known to own or control the property, and where appropriate other interested parties as respondents, who may appear and challenge the forfeiture. If forfeiture is ordered, any of these parties may then appeal under the authority of s. 27 of the *Federal Court Act*. Any interested party who did not receive notice of the forfeiture application may also bring a motion to vary or set aside the forfeiture order within 60 days. The first appeal would be to the Federal Court of Appeal, which has the power to

vary or quash the order, and a subsequent appeal lies, with leave, to the Supreme Court of Canada under the provisions of the *Supreme Court Act*. All of these courts have competence to hear challenges and appeals based on both legal and constitutional issues. To date there have been no appeals relating to terrorist assets, but there have been numerous cases dealing with other criminal assets and applications to challenge seizure and restraint. The most recent notable case was a decision of the Supreme Court of Canada (*Quebec (Attorney General) v. Laroche* [2002] 3 S.C.R. 708)

As of 1 January 2004, there have not been any seizures or forfeitures under these provisions.

Canadian law allows confiscated property to be used to satisfy claims for damages brought by a person or persons who claim to have suffered injuries as a result of the commission of an offence. The relevant *Criminal Code* provision, section 83.14, subsection (5.1), reads as follows:

> Any proceeds that arise from the disposal of property under subsection (5) [property related to terrorist groups or activities as set out in subsection (1), paragraphs (a) and (b)] may be used to compensate victims of terrorist activities and to fund anti-terrorist initiatives in accordance with any regulations made by the Governor-in-Council under subsection (5.2) [distribution of proceeds].

Foreign requests for assistance and the enforcement of foreign orders are dealt with as discussed in the paragraphs dealing with seizure, restraint and forfeiture, above, under authorities set out in the *Mutual Legal Assistance in Criminal Matters Act*. The process is the same as for mutual legal assistance in general: subject to the need for appropriate security measures in respect of terrorism-related cases, a request is submitted to Canada through diplomatic channels and is referred to the appropriate unit of the federal Justice Department. There it is reviewed on legal grounds, supplementary information may be requested, and the matter is referred to the appropriate prosecutorial and law-enforcement or other authorities for action.

In the case of forfeiture, proceeds of the forfeiture are normally disposed of as the relevant (federal or provincial) Attorney General directs, but there is an exception under section 9.4 of the *Mutual Legal Assistance in Criminal Matters Act* for requests to enforce a foreign forfeiture order. In this case the property or proceeds of the disposal are deemed to have been made in favour of the federal government even if the proceedings were brought by a province. This ensures that the property is available for sharing with the requesting foreign state, pursuant to Section 11 of the *Seized Property Management Act*.

1.5 Please indicate whether Canada has ever taken judicial action against a non-profit organization based on that non-profit organization's alleged or suspected involvement in the financing of terrorism? Has Canada ever frozen the assets of any non-profit organizations because of their alleged or suspected links with terrorist groups or terrorist activities?

To date Canada has not taken any specific 'judicial' action against a non-profit organization based on alleged or suspected involvement in the financing of terrorism. However, as indicated later in this

answer, Canada has taken action to list non-profit organizations, freeze their assets, and prohibit fundraising on their behalf.

As indicated in previous reports (S/2003/403 and S/2001/1209), Canada has legislative and administrative mechanisms in place to deal with organizations and individuals that are involved in the financing of terrorism.

Pursuant to Canada's *United Nations Suppression of Terrorism Regulations*, which were created in response to UNSCR1373 and the attacks of September 11, 2001, Canada has listed several international non-profit organizations in concert with other international partners, independent from the Al-Qaida and Taliban Sanctions Committee.

Listing under Canada's *United Nations Suppression of Terrorism Regulations* implements a 'de facto' freeze on the assets of the listed entity in that according to section 4:

> *No person in Canada and no Canadian outside Canada shall knowingly*
>
> *(a) deal directly or indirectly in any property of a listed person, including funds derived or generated from property owned or controlled directly or indirectly by that person;*
> *(b) enter into or facilitate, directly or indirectly, any transaction related to a dealing referred to in paragraph (a);*
> *(c) provide any financial or other related service in respect of the property referred to in paragraph (a); or*
> *(d) make any property or any financial or other related service available, directly or indirectly, for the benefit of a listed person.*

A number of non-profit organizations and charities have been listed in Canada, resulting in the corresponding freezing of assets, including:

Al Aqsa Foundation
Holy Land Foundation for Relief and Development
INTERPAL
Somali International Relief Organization
Wafa Humanitarian Organization.

1.6 Please explain the rules for identifying persons or entities:

which maintain a bank account - When opening an account, financial institutions are required to ascertain the identity of the account holder by referring to an original identification document issued by the federal or a provincial government. Such documents include a passport, birth certificate, driver's license or other similar documents.

When the person is not physically present, the financial institution must confirm that a cheque drawn by the person on an account of a regulated financial institution has cleared, as confirmation that the other financial institution has ascertained the identity of the client.

When the client is an entity, its identity must be ascertained by referring to a document such as the articles of incorporation or a partnership agreement.

on whose behalf a bank account is maintained (i.e. beneficial owners)- When the account is opened, financial institutions and intermediaries are required to determine whether the client is acting on behalf of a third party, and obtain information on the third party (name, address, occupation).

There is no requirement to identify the owners, or shareholders when the client is a company. However, Canada is considering options to comply with the FATF standards in this respect.

who are beneficiaries of transactions conducted by professional intermediaries - Professional intermediaries, including accountants and real estate agents, are required to ascertain the identity of clients who conduct certain transactions in an amount above a prescribed threshold. The third party information requirements mentioned above also apply.

who are connected with a financial transaction - The provisions mentioned above apply. When they conduct certain transactions in an amount above a prescribed threshold, financial institutions or intermediaries are required to determine whether the person conducting the transaction is acting on behalf of a third party, and obtain information on the third party.

Does Canada impose identification obligations on persons, who operate trusts, to obtain information about the trustees, settlers/grantors and beneficiaries of such a trust? Please outline the procedures in place in Canada enabling foreign law enforcement agencies, or other counter-terrorist entities, to obtain this information in cases where terrorism is suspected.

Requirements for trust accounts - When a trust account is opened, the identity of the settlor must be ascertained. For *inter vivos* trusts (i.e., a trust created and coming into existence during the lifetime of the individual at whose instance it has been created), information on the beneficiaries must also be obtained (name, address, occupation).

Information sharing - When FINTRAC has reasonable grounds to suspect that the transaction information it receives is relevant to the investigation or prosecution of a money laundering or terrorist financing offence, it discloses key identifying information to the appropriate law enforcement or intelligence agencies or foreign financial intelligence units (FIUs), pursuant to a Memorandum of Understanding agreed between FINTRAC and the foreign FIU. FINTRAC has concluded information exchange agreements with a number of foreign FIUs and is currently negotiating agreements with additional countries.

1.7 The CTC would be glad to receive a progress report on Bill C-55.

Bill C-17, and its previous iterations (Bill C-55 and C-42), was one of several government initiatives in response to the events of September 11, 2001. It proposed to amend several Acts to maximize Canada's capacity to prevent terrorist attacks. Bill C-17 was progressing through Canada's upper legislative chamber, the Senate, but did not complete the process of review and amendment when the Parliamentary session ended on 12 November 2003. When this occurs, a bill is automatically dropped from further consideration unless the next government decides to re-introduce it.

Bill C-17 was intended to increase the Government's capacity to prevent and to respond swiftly to significant threats or terrorist attacks by:

- Authorizing data collection from air carriers and aviation reservation systems for transmission to federal departments and agencies for the purpose of transportation and national security;
- Allowing for the issuance of interim orders in emergency situations;
- Comprehensively implement *The Biological and Toxin Weapons Convention* (BTWC) such that Canada can fulfill its obligations under the international BTWC more fully with respect to domestic law, ensuring that the Convention's ban is respected not only by the Government of Canada, but also by individuals, organizations and institutions in Canada.

The future of this proposed legislation remains to be determined by the Government.

1.8 Does Canada's counter-terrorist strategy and/or policy targeting (at the national and/or sub-national level) deal with the following forms or aspects of counter-terrorist activity:

Criminal investigation and prosecution

The *Security Offences Act* (SOA) explicitly provides the RCMP with primary responsibility to perform the duties that are assigned to peace officers in relation to "*SOA* section 2 offences" which means any offence or the apprehension of the commission of an offence under any law of Canada where:

a) the alleged offence arises out of conduct constituting a threat to the security of Canada within the meaning of the *Canadian Security Intelligence Service Act*; or,

b) the victim of the alleged offence is an internationally protected person within the meaning of section 2 of the *Criminal Code*.

However, these agreements only establish who performs what task(s) in relation to an incident. It should also be noted that *Criminal Code* offences are broader than SOA offences and that all police jurisdictions have responsibilities with the *Criminal Code*.

Refer to previous reports (S/2002/667 and S/2001/1209) for a description of the RCMP's Integrated National Security Enforcement Teams (INSET) that are specifically designed to address issues related to the investigation of criminal activities that pose a threat to the security of Canada.

Counter-terrorist intelligence (human and technical)

The *Canadian Security Intelligence Service Act* (section 12) gives the Canadian Security Intelligence Service the authority to "collect, by investigation or otherwise" information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada. According to section 2 (c) of the *Act*, "activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political, religious or ideological objective within Canada or a foreign state" constitute a threat to the security of Canada. Together, these sections provide CSIS with the legislative basis to collect counter-terrorist intelligence. Policies and methodologies whereby such intelligence is gathered are confidential.

The *Criminal Code* allows the RCMP to gather information and criminal intelligence by technical means for the expressed purpose of pursuing a criminal prosecution.

Canadian law requires disclosure of information held by prosecutors to defence counsel to ensure a fair trial, but identities and other details of human sources who provide information to law enforcement are protected from disclosure unless the informant actually testifies in court. The relevant law is based on judicial decisions and the case-law has been upheld by the Supreme Court of Canada.

Special forces operations

The Department of National Defence maintains specialized military counter-terrorist forces at high readiness to assist law enforcement agencies in resolving terrorist incidents.

While the Canadian Forces counter-terrorist and hostage rescue force, known as Joint Task Force 2, can be employed in a wide range of special operations roles outside of Canada, its primary mission is to provide armed assistance within Canada. The Minister of Public Safety and Emergency Preparedness, who is the lead Minister for dealing with incidents on Canadian soil, must request use of a military force from the Minister of National Defence. The legal provisions for this call-out are contained in the *National Defence Act* and in a specialized executive order created for that purpose, The *Canadian Forces Armed Assistance Directions*.

Regular liaison and training between military counter-terrorist forces, the Royal Canadian Mounted Police and other law enforcement agencies ensures that the Government of Canada is able to provide a seamless, rapid and effective response to terrorism.

As with all units of the Canadian Forces, when operating in Canada, Joint Task Force 2 supports the efforts of civil authorities while responding to a military chain of command. It operates according to agreed national principles for responding to terrorism as laid out in Canada's National Counter Terrorism Plan. This document includes detailed arrangements for the coordination of military and police responses as well as copies of necessary documents related to the handover of specific (and

limited) responsibilities from police to military commanders during a crisis. The civil authorities maintain overall control of all terrorist incidents in Canada.

When military armed assistance is provided to law enforcement agencies in Canada, the military personnel are subject to Canadian laws and regulations and operate under clear rules of engagement that allow for an effective response while maintaining sacrosanct the rule of law.

Physical protection of potential terrorist targets

The Department of Public Safety and Emergency Preparedness (which includes the former Office of Critical Infrastructure Protection and Emergency Preparedness) has, among its mandates two key responsibilities: to provide national leadership of a new, modern and comprehensive approach to protecting Canada's critical infrastructure - the key physical and cyber components of the Energy and Utilities, Communications and Information Technology, Finance, Health Care, Food, Water, Transportation, Safety, Government, and Manufacturing; and to be the government's primary agency for ensuring national civil emergency preparedness - for all types of emergencies.

Close cooperation and information sharing within the security and intelligence community is essential, particularly in relation to threat assessments for information operations or "cyber warfare", cyber-sabotage and cyber-crime.

The National Critical Infrastructure Assurance Program (NCIAP) is designed to provide a national framework for collaboration by all levels of government in Canada, private industry and our allies and international partners for the assurance of Canada's critical infrastructure. The NCIAP framework is the necessary starting point to achieve a national approach in the following key areas for CIP:

- Policy/strategy development and business/investment decisions;

- Implementation of business continuity and security plans; and,

- Daily execution and operation of security and risk management programs.

The primary objective of the NCIAP is to ensure that Canada's national critical infrastructure is sufficiently resilient, thereby assuring the continued availability of essential services to Canadians. This objective will not be met through a single action or program, but rather through a series of measures taken by the partnership over time.

Strategic analysis and forecasting of emerging threats –

As noted in the 2002 Canadian Security Intelligence Service Public Report, "the primary mandate of CSIS is to collect and analyse information, and to report to and advise the government on threats to the security of Canada." Working in close cooperation with the other operational branches of CSIS, the Research, Analysis and Production Branch (RAP) has the primary responsibility for the analysis, production and distribution of intelligence reports on security intelligence issues of relevance to senior federal decision-makers.

The RAP Branch serves the role of a value-added intermediary between the collection of intelligence and its dissemination to the federal government and law enforcement authorities. RAP analysts utilize their knowledge of regional, national and global trends to assess the quality of collected intelligence and produce insightful security intelligence reports. The Branch produces several types of reports, based upon a broad range of both open-source and classified information, which provide the government with assessments of threats posed by individuals and/or organizations involved in activities prejudicial to the security of Canada.

In addition to the analysis carried out by RAP, in February 2003 the Service established an Integrated National Security Assessments Centre (INSAC), to facilitate collaborative efforts in the analysis and dissemination of intelligence. The INSAC enhances the Service's ability to inform the government of Canada regarding threats to national security.

Analyses of efficiency of anti-terrorist legislation and relevant amendments

The analyses of efficiency of relevant anti-terrorist legislation is an on-going process within Canada. The *Anti-terrorism Act* (Bill C-36) is subject to a legislated comprehensive 3-year review. Section 145 of the *Act* states:

> *Within three years after this Act receives royal assent, a comprehensive review of the provisions and operation of this Act shall be undertaken by such committee of the Senate, of the House of Commons or of both Houses of Parliament as may be designated or established by the Senate or the House of Commons, or by both Houses of Parliament, as the case may be, for that purpose.*

The 3-year review of the legislation has a mandate to recommend changes to the legislation, if appropriate.

The *Act* also requires that two new powers available to law enforcement, recognizance with conditions (preventive arrest) and investigative hearings, be subject to annual reporting requirements. Accordingly, the Attorney General of Canada and Solicitor General of Canada are both required to lay before Parliament annual reports on specific uses of these powers. In addition to the Federal-level reports, the Attorneys General of each province in Canada and the Minister responsible for policing in each in Canada are responsible for making public the same information. Copies of the Federal reports for 2002 can be found at:

> http://www.psepc.gc.ca/national_security/publications_e.asp
> http://canada.justice.gc.ca/en/terrorism/annualreport.html

The federal reports for 2003 are being drafted for public release.

Border and immigration controls

Canada participates in a number of international fora established for the purpose of exchanging information on illegal migration trends and travel document abuse such as the Immigration Fraud Conference, the Pacific Rim Immigration Intelligence Conference, the Inter-Governmental Consultations on Asylum, Refugee and Migration Policies in Europe, North America and Australia (IGC), the G8 and many others. Since 1997, there has been an information sharing arrangement between the US and Canada with respect to suspected terrorists. The *Immigration and Refugee Protection Act* (IRPA) has a number of inadmissibility criteria which have enhanced Canada's ability to control the movement of people across her borders, including security grounds, human rights violations, criminality and organised criminality, as well as misrepresentation.

The following is section 34 of the IRPA, which deals specifically with security concerns:

> *34. (1) A permanent resident or a foreign national is inadmissible on security grounds for*
> *(a) engaging in an act of espionage or an act of subversion against a democratic government, institution or process as they are understood in Canada;*
> *(b) engaging in or instigating the subversion by force of any government;*
> *(c) engaging in terrorism;*
> *(d) being a danger to the security of Canada;*
> *(e) engaging in acts of violence that would or might endanger the lives or safety of persons in Canada; or*
> *(f) being a member of an organisation that there are reasonable grounds to believe engages, has engaged or will engage in acts referred to in paragraph (a), (b) or (c).*

Increased efforts have been made at ports of entry to identify and intercept suspected terrorists attempting to enter Canada. Since September 11, 2001, the Minister of Citizenship and Immigration has introduced measures specifically aimed at further combating terrorism: these measures included the introduction of a more secure identity card for Permanent Residents, initiating security screening for refugees at the outset of the determination process, increased detention capacity, increased deportation capacity, and upgraded security at ports of entry. Additionally, in an effort to deter offences related to the use of fraudulent documents, provisions under IRPA allow for penalties up to a maximum of 14 years.

On December 12, 2003, the Prime Minister announced the creation of the Canada Border Services Agency (CBSA) reporting to the Minister of Public Safety and Emergency Preparedness. The CBSA includes the customs role, portions of immigration enforcement and intelligence and the food inspection agency. The initiation of this new agency will allow for a more co-ordinated approach among partners in managing access to Canada's borders. In addition, it will increase Canada's enforcement capabilities with regard to the prevention of access to Canada by terrorists and other inadmissible foreign nationals.

Control and prevention of the trafficking in drugs, arms, biological and chemical weapons, their precursors and the illicit use of radioactive materials

Canada has an extensive national legislation and enforcement system including the *Controlled Drugs and Substance Act* and its Regulations that addresses illicit drug trafficking in the criminal law context, in full compliance with the UN Drug Conventions.

Control over the export of military and strategically sensitive goods (including those used in the design, development and production of chemical and biological weapons) is exercised through the *Export and Import Permits Act* (EIPA) which allows the creation of the Export Control List (ECL), a list of goods and technologies which can only legally be exported if there is a valid export permit. The list is based on the control lists drawn up by the relevant international control regimes: Wassenaar, Nuclear Suppliers Group, Australia Group, Chemical Weapons Convention.

Exporting without a permit can result in fines or the seizure of the goods by the Canadian Customs and Revenue Agency (CCRA) and in cases of deliberate evasion of the law criminal sanctions of up 10 years imprisonment or an unlimited fine.

Canada has enhanced its nuclear security rules to meet the new threats identified since September 11 2001. Strengthened rules implemented by the Canadian Nuclear Safety Commission apply to radioisotopes and nuclear materials that could potentially be used in a dangerous manner and that could endanger the lives of innocent people. Canada also fully supports and endorses efforts by the G8 and the International Atomic Energy Agency to create international standards for the safety and security of radioactive sources. Canada is working toward full implementation of the Code of Conduct on the Safety and Security of Radioactive Sources adapted in September 2003 and we encourage other countries to do the same. On January 21, 2004, Canada officially informed the IAEA of its support for the Code. Every effort should be made to avoid duplication and to establish harmonization of existing initiatives in this area. Any UN effort for an international implementation should focus on supporting the IAEA's work in this area. We strongly believe the IAEA, given its technical expertise and experience, should remain the leading force behind international efforts in this area. Canada also supports efforts underway at the IAEA to develop guidelines for the Import and Export of Radioactive Sources in accordance with Code of Conduct. These efforts actively support the implementation of UNSCR 1373.

1.9 The CTC would be grateful if Canada could please provide it with information regarding its counter-terrorist efforts including, *inter alia*, an outline of any targeted programs; a list of the agencies involved, and description of any mechanism aimed at ensuring the inter agency coordination in relation to the various areas specified in para 2 and 3 of the Resolution.

The recruitment to terrorist groups

The *Anti-terrorism Act*, among other things, establishes measures to take enforcement action against those responsible for terrorist activities. It also provides law enforcement and national security agencies with new investigative tools.

One integral part of the *Anti-terrorism Act* is the Government's ability to create a list of entities. Under the *Criminal Code*, the Governor in Council may, on the recommendation of the Solicitor General of Canada, establish a list of entities if the Governor in Council is satisfied that there are reasonable grounds to believe that the entity has knowingly carried out, attempted to carry out, participated in or facilitated a terrorist activity; or is knowingly acting on behalf of, at the direction of or in association with an entity that has knowingly carried out, attempted to carry out participated in or facilitated a terrorist activity.

It is the policy of the Government of Canada not to comment on how its law enforcement and security intelligence agencies conduct operations; however, below is the list of terrorist entities (as of January 12, 2004) established for the purposes of Part II.1 of the *Criminal Code*:

- Armed Islamic Group;
- Salafist Group for Call and Combat;
- Al Jihad;
- Vanguards of Conquest;
- Al-Gama'a al-Islamiyya ;
- Al Qaida;
- Al-Ittihad Al-Islam;
- Islamic Army of Aden;
- Harakat ul-Mudjahidin;
- Asbat Al Ansar;
- Palestinian Islamic Jihad;
- Jaish-e-Mohammed;
- Hamas;
- Kurdistan Workers Party;
- Aum Shinrikyo;
- Hizballah;
- Abu Nidal Organization;
- Abu Sayyaf Group;
- Sendero Luminoso;
- Jemaah Islamiyyah;
- Islamic Movement of Uzbekistan ;
- Euskadi Ta Askatasuna;
- Al-Aqsa Martyrs' Brigade ;
- Fuzeras Armadas Revolucionnarias de Colombia ;
- Autodefensas Unidas de Colombia ;
- Ejército de Liberación ;
- Babbar Khalsa;
- Babbar Khalsa International;
- International Sikh Youth Federation;

- Lahkar-e-Tayyivba;
- Lashkar-e-Jhangvi;
- Palestine Liberation Front;
- Popular Front for the Liberation of Palestine; and,
- Popular Front for the Liberation of Palestine – General Command.

A complete listing of those on the *Criminal Code* list can be seen at:
http://www.psepc.gc.ca/national_security/counter-terrorism/AntiTerrorism_e.asp
http://www.psepc-sppcc.gc.ca/national_security/counter-terrorism/Entities_f.asp

The *Anti-terrorism Act* also introduced specific offences related to:

- Financing of terrorism (sections 83.02, 83.03 and 83.04 of the *Criminal Code*);
- Dealing in the assets of a listed entity and not reporting frozen assets to authorities (sections 83.08, 83.1 and 83.11 of the *Criminal Code*);
- Participating in the activities of a terrorist group (section 83.18 of the *Criminal Code*);
- Facilitating a terrorist activity (section 83.19 of the *Criminal Code*);
- Instructing the carrying out of a terrorist activity (sections 83.21 and 83.22 of the *Criminal Code of Canada*); and,

Harbouring or concealing a terrorist (section 83.23 of the *Criminal Code*).

The tracing of links between criminal activity (in particular, drug trafficking and terrorism)

Canada has a number of mechanisms and structures in place to ensure inter-agency cooperation between authorities responsible for curbing drug trafficking, financial tracking and security. There are existing intelligence and security, and law enforcement agreements and memoranda of understanding between a number of Canadian agencies including CBSA, CSIS, RCMP and FINTRAC as well as international agreements relating to border security.

Please refer to previous report (S/2002/667) for a description of specific inter-agency coordination/operational mechanisms such as the Enforcement Information Index (EII), Integrated National Security Enforcement Teams (INSETS), Integrated Justice Information Initiative (IJII), Canada Public Safety Network (CPSN) and Integrated Border Enforcement Teams (IBETS).

The denial of safe havens to terrorists, as well as the denial of forms of passive or active support for terrorists or terrorists groups, including *inter alia*; logistical support for terrorists (e.g. the use of global information infrastructure)

It is the role of both Citizenship & Immigration Canada (CIC) and the CBSA to ensure, in co-operation with other partners, that foreign nationals wishing to enter Canada meet the admissibility criteria as set out in IRPA. For example, persons applying for Permanent Resident or Convention Refugee status are security screened, as are some temporary residents (visitors).

CSIS, an important partner for both CIC and the CBSA, provides input to a database which alerts Immigration and Customs officers at ports of entry of threats to national security posed by suspected and known terrorists seeking admission to Canada. CSIS information enables Canadian officials to refuse applications from individuals suspected of involvement in terrorist activity, effectively barring their entry into Canada.

The CBSA plays a leading role in protecting the integrity of Canada's immigration and refugee system, and in denying safe have to persons suspected of terrorism. The CBSA identifies, detains, and removes persons who are ineligible to remain in Canada for security or criminality reasons (including terrorism) or those who have been determined not to be Convention refugees.

Canada has initiated procedures whereby airline passenger manifest information is electronically transmitted to the Ports of Entry in advance of the arrival of the flight. This provides the CBSA officials with the opportunity to identify individuals who may warrant further examination upon arrival.

The CBSA and the United States Department of Homeland Security have a co-ordinated approach to border management by sharing passenger flight information, within the limits of their respective privacy legislation. The National Risk Assessment Centre (NRAC) has been established to allow Canada and the United States to detect and interdict high-risk travellers destined to either country. The NRAC became operational in January of 2004.

1.10 Please indicate which special investigative techniques can be used in Canada in cases of terrorism (e.g. interception of communications; electronic surveillance; observation; undercover operations; controlled delivery; "pseudo-purchases" or electronic bugging of private of public premises etc.). Please indicate whether these techniques may 1) only be applied against suspects; 2) only be applied if approved by a court.

Canadian law-enforcement and security agencies have access to a full range of special investigative techniques in terrorism-related cases, depending on the facts of each case, the type of investigation involved, and the agency conducting the investigation. Available techniques include electronic surveillance, search and seizure, personal or "undercover" surveillance, use of anonymous informants, and controlled delivery or other conduct by investigators that would in other circumstances constitute a criminal offence. Specific legal authorities are found in a number of statutes and in case law, but the principal provisions are the *Canadian Charter of Rights and Freedoms*, the *Criminal Code* (Part VI dealing with electronic surveillance, Part XV, dealing with search and seizure, and sections 25-25.4 dealing with justification of otherwise illegal acts for investigative purposes). With the exception of electronic surveillance in criminal cases (below) all of these investigative powers may be used in cooperation with another State pursuant to a mutual legal assistance request in criminal matters or another agreement or arrangement in security matters.

The use of special investigative techniques in Canada is circumscribed by substantive and procedural safeguards. Different standards apply depending on whether the investigation is conducted by a law enforcement agency for the purposes of prosecuting a criminal or other offence, or by a security

agency for national security purposes, and within the general legal frameworks, vary depending on the technique to be used and the circumstances in which it will be used. Underlying all of the specific legal authorities and safeguards is the *Canadian Charter of Rights and Freedoms*. This includes the right of everyone in Canada to be secure against unreasonable search or seizure, which in the case of electronic surveillance and conventional search and seizure cases, requires that operations meet basic standards for justification. These are that the search or surveillance operation be authorized in advance by an independent judicial officer who, where appropriate, may set limits on what may be done and how it may be done. There is a limited exception to this basic rule for emergency or "exigent" circumstances. Other rights, particularly those providing for fairness in criminal proceedings, require disclosure of potentially sensitive information to accused persons, but the ultimate remedy in such cases is not disclosure but the discontinuation of the prosecution where the information cannot be disclosed.

Electronic surveillance - In Canada, the term "interception of private communications" includes all forms of electronic surveillance whether the communication is intercepted in transit through a communications system or network or by the use of electronic means to eavesdrop on a fixed conversation. If a reasonable expectation of privacy exists on the part of the communicants, then interception is a criminal offence unless an exception is provided by law.

Part VI of the *Criminal Code* allows for electronic surveillance to investigate criminal offences listed in the legislation, provided that prior judicial authorization is obtained. The list of eligible offences includes all serious criminal offences and all of the offences designated as "terrorist activities" in the legislation. Judicial authorizations may only be issued to specially-trained officers, and limits on duration and physical scope are established both in the legislation and by the court. There is a requirement that electronic surveillance only be used as a last resort when other means have failed or are unlikely to succeed for ordinary criminal offences, but this does not apply offences involving a criminal organization or a terrorism offence. The normal maximum period for which electronic surveillance can be authorized is 60 days, but in the case of a terrorism offence, this is increased to one year, and in both cases judges may renew the authorization as necessary where circumstances warrant. Short-term authorizations can also be obtained quickly, in emergency or "exigent" circumstances.

The *Canadian Security Intelligence Service Act* provides separate powers to conduct electronic surveillance. Warrants under the *Act* must also be obtained from a judge, but are obtainable on the more general basis of an investigation of threats to the security of Canada or the performance of other duties and functions described in the *Act*. Only designated judges of the Federal Court of Canada may issue warrants under the *Act*, and unlike *Criminal Code* procedures, warrants under the *Act* may deal with either electronic surveillance, search and seizure, or both. The period for which a warrant to intercept communications can be issued is 60 days or one year, depending on the nature of the investigation, and can be renewed where circumstances warrant. The Communications Security Establishment, which gathers signals intelligence from the global information infrastructure and advises the Government of Canada on communications security, also has electronic surveillance powers.

Electronic surveillance under both the *Criminal Code* and the *Canadian Security Intelligence Service Act* can be directed at known persons or unknown persons, provided that there is a sufficient degree of specificity in the information provided to the issuing judge and included in the warrant or authorization to limit the scope of the surveillance. It may also be directed at any place, provided that the place is described with sufficient specificity, including private "dwelling houses" and more public places. Additional safeguards are applied where the communications to be intercepted under the *Criminal Code* may be privileged solicitor-client communications. Depending on circumstances, if a place is sufficiently public or if communicants are notified in advance, there may be no expectation of privacy, and hence no legal restrictions on recording communications. Electronic surveillance under the *Criminal Code* is limited to the investigation of Canadian offences listed in the *Code*. This includes terrorist and other offences committed on Canadian aircraft or vessels, or committed elsewhere but deemed to have been committed in Canada, but does not include mutual legal assistance requests relating to offences committed in other countries. Electronic surveillance by the Canadian Security Intelligence Service is based on the investigation of threats to the security of Canada or the collection of intelligence or information and this may involve cooperation with other States where appropriate. Provisions under both statutes allow for measures to keep confidential the identities of informants (see below) and other sensitive information used by the judge in issuing the authorization or warrant.

Search and seizure - Canadian law enforcement agencies have powers to search for and seize anything that may be evidence in a criminal case, and a range of other specific items, including proceeds of crime and other offence-related property, weapons, narcotic drugs and psychotropic substances, various contraband items, and nuclear materials. General search and seizure powers relating to evidence are contained in the *Criminal Code*, with subject-specific powers in the *Criminal Code* and other statutes. Prior judicial approval based on appropriate grounds and setting out what may be search for and seized, where and other limits is normally required, but there are limited powers to search without a warrant in emergency or exigent circumstances. The Canadian Security and Intelligence Service may search for and remove or return, examine, take extracts from, make copies of, or record in any other manner, any information, record, document or thing. This may be done based on the same justification and subject to the same limitations as for electronic surveillance.

Use of undercover officers - There is no legal restriction on the conduct of law enforcement or security operations in plain-clothes or out of uniform, or on the ability of officers to pretend to be involved in unlawful activities for the purpose of gathering intelligence or evidence. Individual agencies have internal orders or guidelines governing the conduct of specific types of operations, but these do not restrict overall use of the techniques.

Anonymity and protection of informant - Canadian law enforcement and security agencies are able to preserve the anonymity of informants where necessary. This is done using administrative means and generally only becomes a legal issue where the informant's information is used as the basis for obtaining a search warrant or authorization to conduct electronic surveillance. In such cases, the normal rule is that legal counsel for the defence would have a right to review sworn documents and cross-examine the principal informant, who is usually an investigator, but there is no right to cross-examine a confidential informant. Where anonymity is necessary, documents used to obtain general

search warrants under the *Criminal Code* can be ordered sealed by a court. Documents used to obtain an electronic surveillance authorization under the *Criminal Code* are sealed, and if given to defence counsel, are edited by a judge to remove the identities of confidential informants, as well as any other information that might identify them. Investigative techniques conducted under warrants pursuant to the *Canadian Security Intelligence Act* are not used in criminal cases and the question of access by defence counsel does not arise. Warrants are issued by designated judges of the Federal Court of Canada and are subject to independent confidential review only. All of the measures whereby the identity of informants and other information can be shielded from disclosure are subject to the rights guaranteed to persons accused of criminal offences. Where lack of access to sensitive information amounts to a deprivation of rights under *The Canadian Charter of Rights and Freedoms* and this deprivation is not done in accordance with the principles of fundamental justice, remedies may include a stay of prosecution.

Use of controlled delivery and "pseudo-offences" - Canada's *Criminal Code* was amended in 2001 to clarify that law enforcement officers and others may engage in conduct that would otherwise constitute a criminal offence for investigative purposes, provided certain conditions are met. Actions such as controlled delivery of illicit substances may be done only by officers who are trained and designated, and operations must be approved in advance by a senior official. The exception operates as a justification and does not convey complete immunity: actions taken must be reasonable and proportional, having regard to the offence being investigated; the exception does not extend to the commission of offences causing death, sexual offences or the obstruction of justice, and a separate regime exists for narcotics offences. The justification provision extends to any "public officer" who has been designated, which may include officers of federal, provincial and municipal police forces, the Canadian Security Intelligence Service, and other departments or agencies of the federal government or a provincial government with investigative or law enforcement mandates. The justification also extends to actions by persons who are not "public officers", such as civilian informants, on a more limited basis. The person taking the action must reasonably believe that he or she has been directed to do the act by a public officer who has the authority to do so, and the act is done for the purposes of the public officer's law enforcement duties.

Cross-border pursuits - Canadian legislation does not provide extraterritorial powers for Canadian law-enforcement personnel in pursuits into other countries or powers or protections for foreign personnel entering Canada. "Hot-pursuit" scenarios do occur on the border between Canada and the United States, and these are dealt with in accordance with arrangements between the law-enforcement authorities involved and, if necessary, prosecutorial discretion. Should an arrest be necessary to prevent flight or further harm, a foreign law-enforcement officer who has crossed into Canada would have the same powers as a Canadian civilian. A person found committing a serious offence or who is being pursued may be arrested and reasonable force may be used, provided that the person arrested is turned over to a Canadian peace officer forthwith.

Entrapment - Canadian criminal investigators are permitted to mislead or deceive suspects, but entrapment will give rise to a valid defence to criminal charges. In Canadian law, entrapment occurs when investigators actively encourage or induce a suspect to commit an offence, or merely provide an

opportunity to commit the offence and there is no reasonable suspicion of improper motive or criminality on the part of the suspect.

Law enforcement and security and intelligence agencies have a variety of special investigative techniques available to them through legislation. The granting of all the special investigative powers must be sanctioned by the judiciary.

It is the policy of the Government of Canada not to comment on how its law enforcement and security intelligence agencies conduct operations or use any of the special investigative techniques available to them through legislation.

1.11 With a view to bringing terrorist and their supporters to justice, please indicate whether Canada has taken measures to protect vulnerable targets in terrorist cases, for example, to protect victims, witnesses or other persons assisting the court, judges and prosecutors. Please describe the legal and administrative provisions that Canada has put in place to ensure this protection. Could Canada please outline whether these measures can be utilised in cooperation with or at the request of another State.

Under Canada's *Witness protection Program Act*, a full range of measures needed to protect vulnerable persons is available. These provisions are equally applicable to those whose circumstances involve terrorism-related matters as to proceedings relating to any other offence. Anyone who participates or has agreed to participate in a criminal proceeding may be protected, as well as others, such as family members, likely to be in danger. The *Act* also provides for reciprocal agreements or arrangements with other countries under which subjects in Canada may be relocated abroad and those in other countries may be relocated in Canada. Canada considers foreign requests under this provision on a case-by-case basis. The *Act* establishes the conditions needed for formal, long-term protection programmes, as well as emergency measures pending the application of the long-term provisions. It should also be noted that for most of the immediate measures needed to protect witnesses, other participants or others who may be in danger, no specific legal authority is required. Canadian law-enforcement agencies can and do take appropriate measures where deemed necessary.

Canada's Federal Witness Protection Program is administered by the RCMP. Provincial and municipal agencies also maintain witness protection programs, with federal assistance in obtaining documents where necessary. The RCMP works with other federal departments in order to facilitate the obtaining federal documents for witnesses who have undergone secure changes of identity. Witnesses are usually entered into the program upon completion of the investigation, at which time the identity of the witness will usually become known to the accused as part of legally-required pre-trial disclosure. However, should a threat be identified at any other time, a witness can at that time be entered into the program, either under emergency provisions or the regular admittance procedures. The 2001 *Anti-terrorism Act* amendments allow for non-disclosure of sensitive or potentially injurious information, which would include in appropriate circumstances information that would identify an informant or witness. Where the witness actually testifies, it is not possible to do so anonymously, and in cases where disclosure of information is blocked, the court will fashion a remedy to ensure that the accused's right to a fair trial is protected.

Protective measures are based on a threat assessment and can include personal protection and the removal of the subject from the threat area until the threat subsides. In more serious cases, the subject is relocated and provided with a change of identity. The relocation includes handler support at the relocation site. Assistance with obtaining secure accommodations and counselling are available where necessary.

1.12 The CTC would be grateful for an outline of Canadian legal procedures and administrative mechanisms with a view to ensuring adequate cooperation and information sharing among the different government agencies that may be involved in the investigation of terrorist activities, with particular regard to the financing of terrorism. Do the legal provision in place authorize the administrative authorities to share both public and non-public information concerning counter-terrorism with their domestic and foreign counterparts?

Canada has undertaken to establish administrative procedures for the sharing of information in relation to terrorist financing initiatives. Law enforcement and security and intelligence agencies have existing mechanisms, both legislative and administrative, for sharing information domestically and with international partners.

Originally established to facilitate the process for listing entities and freezing assets, an interdepartmental committee comprised of numerous departments and agencies exists and meets on a regular basis that has expanded its role to include the sharing of information and strategies related to the listing of entities and freezing of assets, as well as identifying policy and program gaps in relation to efforts to combat terrorist financing.

Canada is also an active member in various international bodies and organizations that address the issue of terrorist financing. In order to ensure a coordinated national approach in these various fora, interdepartmental meetings and consultations occur regularly among delegation members.

Under prescribed conditions, FINTRAC may disclose designated information derived from its analysis of the reports received and other information received or collected such as through both public and governmental databases. (Designated information can be categorized as 1) identifying information about the individual or company involved (including account information), 2) details of the transactions, and 3) details about the institutions where the transactions took place.)

- The Centre must disclose to the appropriate police force when it has reasonable grounds to suspect that this information would be relevant to the investigation or prosecution of a money laundering or a terrorist financing offence.
- The Centre must disclose to CSIS when it has reasonable grounds to suspect that the information would be relevant to threats to the security of Canada.

Once the threshold of reasonable grounds to suspect money laundering or terrorist financing is met, FINTRAC must also disclose such designated information to:

- The Canada Customs and Revenue Agency (CCRA), when the information is also determined to be relevant to an offence of evading or attempting to evade federal taxes or duties;
- Citizenship and Immigration Canada (CIC)*, when the information is also determined to be relevant to certain provisions of the *Immigration and Refugee Protection Act*; and
- Foreign FIUs with which it has concluded a memorandum of understanding (MOU) providing for such exchange of information. FINTRAC may also query FIUs for additional information where an MOU is in place. FINTRAC has concluded MOUs with the United States, United Kingdom, Mexico, Belgium, Australia, Barbados and Italy.

Once information is disclosed by FINTRAC, it is no longer subject to the requirements of the PCMLTFA, but would still be subject to any legal restrictions applicable to the agency or department to which it was disclosed, including the Privacy Act and, where applicable, the Security of Information Act.

Canada's public administration includes a number of departments and agencies that are involved in the prevention and investigation of terrorism and related subject-matter, at the federal, provincial and local levels of government. These include law enforcement and national security agencies, federal and provincial attorneys-general, and federal and/or provincial departments responsible for health, transportation, immigration and other matters. Within this structure a number of different arrangements exist for the consultation and sharing of information with other relevant departments. These range from committees formally established by legislation or delegated legislative powers, to informal and ad-hoc arrangements established to share information or cooperate as necessary on a case-by-case basis. Interdepartmental committees and working groups include a number of federal-provincial bodies dealing with both policy and operational subject-matter.

In Canadian law, information that is held by any government agency falls into one of three basic categories. Public information, which comes from open sources such as the mass-media and public statements of officials, is widely disseminated and not subject to legal restrictions. The other two categories, personal information and secure information, involve varying degrees of sensitivity and are subject to legal provisions which prohibit publication or dissemination and establish exceptions for a range of circumstance in which they can be shared. Within this general framework, a number of specific non-disclosure provisions exist in Canadian statutes. These establish rules governing specific types of information, establishing to whom it may be disclosed and under what circumstances, but most are unlikely to apply in terrorism-related cases.

Regarding public information, most government departments have open Internet web-sites from which information about their mandates and initiatives can be reviewed and downloaded, including the RCMP and CSIS. These are used to disseminate public research, consult with Canadians and provide basic information about the agencies, what they do, and how they can be contacted. Both the RCMP and CSIS websites also provide information about how to contact their respective independent review bodies in order to register concerns or file specific complaints. All government departments also have media-relations offices established for the purpose of transmitting information to the mass-media and general Public Communications.

Personal information, which consists of information about identifiable individuals held by government institutions, raises privacy issues and is subject to the federal *Privacy Act*, or similar regimes that exist in the provinces and territories. Such information can be gathered and retained by an agency for specific purposes, but can only be used for other purposes or disclosed to other agencies with the consent of the subject, or in circumstances specified in the *Act*. Circumstances where information can be shared include: information disclosed on the order of a court; information disclosed to an investigative body or for legal proceedings; and information disclosed pursuant to an agreement or arrangement between the Government of Canada and a province, another country, or an intergovernmental organization "...for the purpose of administering or enforcing any law or carrying out a lawful investigation".

Secure information, the disclosure of which would be prejudicial to the safety or essential interests of the State, is further protected by the *Security of Information Act*. Sharing of this information can be authorized and takes place in appropriate circumstances, including terrorism-related cases. Federal laws governing specific agencies in some cases then establish more specific frameworks for information practices that apply only to the agencies involved and the information in their possession. The rules governing the RCMP, CSIS, and the FINTRAC are relevant in this context.

Information gathered and held by the RCMP is dealt with in accordance with the provisions of the *Privacy Act*. Information gathered and held by CSIS is subject to section 19 of the *Canadian Security Intelligence Service Act*, which prohibits disclosure except under specific circumstances, which are specified in the *Act*. Information can be disclosed for the purposes of the performance of CSIS' duties and functions under the *Act*. Information can also be disclosed for other purposes including the investigation and prosecution of offences, matters relating to foreign relations or national defence. It may also be disclosed more broadly within the public service where such disclosure is determined by the Solicitor General to be essential in the public interest and where the interest in such disclosure clearly outweighs any consequent invasion of privacy. Some research studies do not raise privacy or security issues and an extensive collection of these studies on a number of topics, including terrorism, are disseminated by CSIS on its website.

Canada's constitutional bill of rights, the *Canadian Charter of Rights and Freedoms*, also establishes privacy rights that regulate the gathering and use of information and with whom and for what purposes it may be shared. Exact standards depend to a large degree on specific circumstances, but generally, if there is a reasonable expectation of privacy for information, there will be restrictions on how it must be gathered, such as requirements that activities such as electronic surveillance and search and seizure must be authorized by an independent judicial officer in advance. There will also be limits on disclosure and use, and in some cases, information gathered for one justified purpose may not be further used or disclosed for other purposes, or may be subject to requirements for further review of other safeguards before this is done. These must be prescribed by law. Under Canada's anti-terrorism legislation, for example, individuals may be ordered by a court to appear and disclose information at investigative hearings, if there are reasonable grounds to believe that a terrorism offence has been or will be committed, but this process is not permitted for ordinary criminal investigations, and any information generated under these circumstances cannot later be used in a

criminal prosecution against the person compelled to provide it. The legislative and administrative frameworks for sharing information in Canada are consistent with these basic *Charter* principles, and new legislative proposals are reviewed for consistency before they are introduced in Parliament. The sharing or disclosure of information in exigent (emergency) circumstances is also provided for by Canadian law.

Modern information technologies play a significant and increasing role in information-sharing in Canada. As noted, most Canadian government departments and agencies now maintain open Internet web-sites. These provide a means of widely disseminating information, and most also provide information about how the department or agency itself, and its independent oversight body, if any, can be contacted. Some also provide for return communication by electronic mail, using appropriate encryption technologies to protect privacy and security. As Internet security technologies improve, secure web-sites and electronic mail networks are sometimes used to share more sensitive information. One such major Canadian network is the Canadian Police Information Centre (CPIC), which has been operated since 1972 by the Royal Canadian Mounted Police. It maintains a secure database containing law-enforcement information that is accessible by all Canadian police agencies and other approved federal and provincial law-enforcement agencies. Its databases can be queried for information about persons of interest, vehicles and other information, new information can be added to the system, and participants can exchange information bilaterally in a secure environment. CPIC is presently undergoing a major modernization programme to expand its capabilities and include non-police agencies that require the information it contains, including agencies responsible for customs and immigration matters.

Other more narrowly-focused databases, websites and other facilities exist, employing appropriate security measures, for sharing information among departments, agencies, or individual officials who need the information. The majority of these allow users to both send and receive information. Many of them, including CPIC, are accessible to appropriate officials at the federal, provincial, and municipal levels, and some are accessible to appropriate foreign law enforcement agencies or other authorities.

Canadian legal procedures and administrative mechanisms relating to co-operation and information-sharing between Canadian government agencies involved in the investigation of terrorist activities and their foreign counterparts, with particular regard to the financing of terrorism -

The sharing of information with public officials of other countries is generally governed by the same legal principles protecting privacy and regulating disclosure as domestic information. In addition, it is regulated by international legal instruments to which Canada is a State Party, and by the discretionary application of the principles of state sovereignty, essential interests and reciprocity. Treaties are not self-executing in Canada and must therefore be implemented by appropriate legislative and administrative measures. Canada is a State Party to the United Nations Convention against Transnational Organized Crime and all of the 12 international legal instruments against terrorism, and shares information as required under the frameworks set out in those treaties.

As noted, some web-sites and other communications facilities established by Canada are made accessible to foreign agencies, and Canadian officials have and use access to similar sites established by other countries, subject to the need for appropriate security measures. A major concern for Canada is the security of the border between Canada and the United States of America and travel between the two countries, and numerous bilateral mechanisms have been established to facilitate information-sharing in that context. Information-sharing initiatives are established with other countries and regional or other intergovernmental organizations, including the International Criminal Police Organization (INTERPOL) as necessary and appropriate.

Canadian legal procedures and administrative mechanisms governing the sharing of public and non-public information -

As noted above, information held by the Government of Canada is only restricted if it is personal information within the ambit of the *Privacy Act*, secure information within the ambit of the *Security of Information Act*, or personal information in which there is a reasonable expectation of privacy under the *Canadian Charter of Rights and Freedoms*. Subject to specific legal non-disclosure rules, other information would generally be considered as public information and there would be no restriction on its disclosure or dissemination.

1.13 The CTC notes from sub-section 3.74 of Bill C36 that Canadian courts would not appear to have jurisdiction over a foreign national who is accused of having committed an act of terrorism abroad when he was present in Canada (but not resident) in Canada. Please outline how Canada would deal with a foreign national who is present in Canada and is suspected of having committed a terrorist act abroad, in light of the prosecute or extradite" (*aut dedere aut judicare*) principle of international law.

Canada has established the necessary jurisdiction in respect of those offences for which it is required to implement the principle of *aut dedere aut judicare* by its obligations under international legal instruments, including the relevant conventions and protocols against terrorism. It is Canada's position that, generally, extended or universal jurisdiction should only be applied in accordance with international law as set out in the relevant treaties, and the legislation therefore only assumes jurisdiction to the extent required for each offence by each international instrument.

As a general rule, the specific offence provisions are added to the appropriate chapters of the *Criminal Code*, depending on the type of conduct being criminalized as required by each treaty. The jurisdiction to prosecute persons accused of these offences where Canada is obliged to prosecute or extradite and does not extradite is found for each such offence in the appropriate subsection of section 7 of the *Criminal Code*. Each subsection establishes the jurisdiction required by the international legal instrument concerned. In the case of terrorism offences, these are the offences listed in sub-paragraph (a) of the definition of "terrorist activity" in *Criminal Code* subsection 83.01(1). These offences are excluded from the general jurisdictional provision found in section 7, subsection 3.74 of the *Criminal Code*, which applies only in respect of offences that are not the subject of any international legal instrument, and for which the *aut dedere aut judicare* obligations do not apply. This is because the relevant jurisdictional rules are found in section 7, subsection (3.73) instead.

In the case of an offence enacted pursuant to the *International Convention for the Suppression of the Financing of Terrorism*, for example, the offence itself is found in *Criminal Code* section 83.02. It is listed as a form of "terrorist activity" in section 83.01, subparagraph (1)(a)(x), which excludes it from section 7, subsection 3.74. The correct jurisdictional provision, section 7, subsection (3.73), establishes jurisdiction in a series of listed circumstances, including, under subparagraph (d), "...the person who commits the act or omission is, after its commission, present in Canada." Similar provisions implement the jurisdictional requirements established by the other conventions and protocols against terrorism.

1.14 Please indicate whether Canada has taken measures to establish the civil, criminal or administrative liability of legal persons for criminal offences, in particular offences related to terrorist activities? Please specify and provide an outline of the relevant legal documentation. Is it possible to assign liability to a legal person, in cases where no natural person has been identified or convicted? In this regard could Canada provide the CTC with statistics of the number of cases where sanctions, for the provision of support to terrorists or terrorist organizations, were imposed on: non-profit organizations; financial and non-financial institutions; and other financial intermediaries.

Canada has not prosecuted a non-profit organization for providing support to terrorists or terrorist organizations.

Section 2 of Canada's *Criminal Code* provides that the terms "every one", "person", "owner" and similar expressions include a range of legal persons. This means that legal persons are subject to full liability for all criminal offences in which these basic terms are used. The effect is that they are fully subject to all criminal offences in Canada unless the specific enactment that establishes the offence provides otherwise. They are fully subject to liability for all of the offences directed specifically at terrorist activities, as well as all offences of general application, such as homicide offences, which might arise in relation to terrorist activities. If convicted, they are subject to punishment in the form of a fine.

In 2003, the relevant *Criminal Code* provisions were amended to provide a clearer and more comprehensive provision governing the scope of criminal liability and the types of organization to which it extends. The changes specifically include a number of additional types of organization, whether operated on a profit-making or non-profit basis. The amendments are contained in Bill C-45 (now S.C. 2003, c.21), *An Act to amend the Criminal Code (criminal liability of organizations)*.

As amended, the relevant *Criminal Code* provisions are as follow.

Section 2 (definitions) was amended to read (in part):

In this Act,

``every one", ``person" and ``owner", and similar expressions, include Her Majesty and an organization;

``organization" means
(a) a public body, body corporate, society, company, firm, partnership, trade union or municipality, or
(b) an association of persons that
(i) is created for a common purpose,
(ii) has an operational structure, and
(iii) holds itself out to the public as an association of persons;

New sections 22.1 and 22.2 were enacted to detail the rules for attributing criminal liability to legal persons for offences of criminal negligence and offences requiring subjective intent, respectively:

22.1 *In respect of an offence that requires the prosecution to prove negligence, an organization is a party to the offence if*
(a) acting within the scope of their authority
(i) one of its representatives is a party to the offence, or
(ii) two or more of its representatives engage in conduct, whether by act or omission, such that, if it had been the conduct of only one representative, that representative would have been a party to the offence; and
(b) the senior officer who is responsible for the aspect of the organization's activities that is relevant to the offence departs - or the senior officers, collectively, depart - markedly from the standard of care that, in the circumstances, could reasonably be expected to prevent a representative of the organization from being a party to the offence.

22.2 *In respect of an offence that requires the prosecution to prove fault - other than negligence - an organization is a party to the offence if, with the intent at least in part to benefit the organization, one of its senior officers*
(a) acting within the scope of their authority, is a party to the offence;
(b) having the mental state required to be a party to the offence and acting within the scope of their authority, directs the work of other representatives of the organization so that they do the act or make the omission specified in the offence; or
(c) knowing that a representative of the organization is or is about to be a party to the offence, does not take all reasonable measures to stop them from being a party to the offence.

The new legislation also increases the amount of fine available for an organization convicted of a summary conviction offence. Fines for indictable offences have no upper limit. There is also provision for probation with conditions for an organization.

Whether a legal person or those who act on its behalf are actually held liable is a question of fact to be adjudicated on a case by case basis. There is no legal bar to a legal person and a natural person being convicted for the same offence, and both or all parties would be convicted where the trier of fact finds against each of the accused on all of the essential elements of the offence involved. A legal person

can also be convicted in a case where no natural person is prosecuted, or where a natural person is prosecuted but not convicted of the same offence. The authorities on these issues are primarily case law, based on English common-law and sections 2, 21, 22.1 and 22.2 of the *Criminal Code*, as amended. The leading case on corporate liability generally is *R. v. Canadian Dredge and Dock Co.* [1985] 1 S.C.R. 662 (Supreme Court of Canada). The leading case dealing with the liability of both natural and legal persons in the same case is *R. v. Fell* (1981), 64 C.C.C. (2nd) 456, 131 D.L.R. (3rd) 105 (Ontario Court of Appeal).

Legal persons in Canada are subject to liability for many administrative and regulatory offences, including a number that enforce banking, financial and corporate governance requirements outside of the scope of the criminal law. Generally, these carry lesser punishments, and require a lower standard of *mens rea* than do criminal offences, such as requirements that regulated entities not be negligent or requirements that due diligence be exercised in meeting prescribed legal obligations.

Regarding civil liability, there is no civil liability in tort for criminal offences relating specifically to terrorism. However, civil actions framed in tort may be brought to deal with terrorism activities. For example, bribery may be indicative of the tort of conspiracy.[1] Other torts may also provide the basis for a civil action to deal with terrorism, such as the tort of unlawful interference with an economic interest or the tort of deceit.

1.15 Could Canada please provide the CTC with information relating to the number of persons prosecuted for terrorist activities; the financing of terrorist activities; recruiting to terrorist organizations; and providing or inviting support for terrorists or terrorist organizations.

Canada's system for recording criminal justice statistics is based on classification according to the offences prescribed by Canadian law, and until the adoption of the offences contained in the *Anti-terrorism Act* in December 2001, no Canadian criminal offences contained terrorism per se as an element. Terrorism-related categories were automatically incorporated following adoption of the Act, but as of 31 December 2003, no prosecutions had been recorded by the Canadian Centre for Justice Statistics, and officials are not aware of any ongoing prosecutions. A definitive response on this point would require further consultation with provincial Attorneys-General, who have concurrent jurisdiction with the federal Attorney-General over these offences, but it is unlikely that any such prosecutions are ongoing or would be undertaken by a province without consultation with federal officials.

Prior to the adoption of the 2001 offences, terrorism-related prosecutions in Canada, when they occurred, would have been dealt with as the appropriate substantive offences, such as murder or hostage-taking. One major homicide prosecution, arising out of the destruction of an Air-India flight from Canada to India via the United Kingdom and the deaths of 329 persons, in June 1985, was

[1] In Canada, a conspiracy is actionable in tort where two or more persons 1) combine to act unlawfully with the predominating purpose of injuring the plaintiff, 2) combine lawfully with the predominating purpose of injuring the plaintiff or, 3) combine to act unlawfully and their conduct is directed towards the plaintiff and the likelihood of injury to the plaintiff is known or should be known to the defendants.

commenced in 2003 and was still before the courts as of 31 December 2003. Officials are aware of a very small number of other incidents since 1980 where offences were committed for terrorist or political motives. From 1991-1996, the Canadian Centre for Justice Statistics included the category "terrorism-related" in its survey protocols for homicide incidents, but no incidents were recorded, and the classification was abandoned as not statistically relevant. Since then, it has sought information about "terrorism, political cause" as a form of motive, and only one such incident was recorded between 1997-2002, the most recent year for which statistics are available (Not all Canadian provinces reported on this question, but the data is believed to represent about 80% of the total.)

1.16 Could Canada please provide the CTC with an outline of the procedure used to enlist an organization as a terrorist organization? Could Canada provide data on the number of terrorist organizations that it has so listed, in particular foreign terrorist organizations other than those listed by the Security Council? How long does it take to list a terrorist organization at the request of or based on the information of another State? How many persons (legal or physical) have been prosecuted for inviting support (including recruitment for) proscribed organizations and other terrorist groups of organizations?

The *United Nations Suppression of Terrorism Regulations* allow Canada's executive authority, the Governor in Council, to establish a list of entities where there are reasonable grounds to believe a person (individual or entity) has carried out, attempted to carry out, participated in or facilitated the carrying out of a terrorist activity, or is controlled directly or indirectly by such a person, or is acting on behalf of, or at the direction of, or in association with such a person. Information considered during the Governor in Council process is protected from disclosure.

The administrative process for preparing and proposing persons for listing considerations to the Governor in Council involves the production of a report by security intelligence designed to meet the test for listing established in the Regulations and appropriate consultation prior to the Governor in Council consideration. As part of the international cooperation against terrorism, the process may be initiated when a specific request is made to Canada by another State to take action to freeze the assets of a specific entity. In such a case, the information provided to Canada by another State in support of a listing is reviewed and assessed by the appropriate security intelligence agency that also conducts its own investigation. Canada will advise the requesting State if the information provided is insufficient to meet the standard for listing established in the Regulations. Canada seeks to list promptly upon receipt of a request by another State if the standard for listing is met in order to block the transfer of assets to Canada from other States that have taken action against an entity. The length of time for a listing can vary depending on the urgency of the matter and the information provided to Canada in support of a listing. Efforts are made to list in concert with our international partners when possible.

The *UN Suppression of Terrorism Regulations* also incorporate by reference the foreign terrorist organizations listed by the Security Council. There are currently 56 persons listed, both individuals and entities, that are not listed by the Al Qaida and Taliban Sanctions Committee. Of these, 19 are also listed under Criminal Code.

Section 83.05 of the *Criminal Code* allows the Governor in Council to establish a list of entities where there are reasonable grounds to believe the entity knowingly participated in or facilitated a terrorist activity as defined by the *Criminal Code*.

Information considered during the Governor in Council process is protected from disclosure. However, the administrative process for preparing and proposing entities for a listing consideration to Governor in Council involves the production of a detailed security intelligence/ criminal-report designed to meet the test for listing established in the *Criminal Code* and appropriate consultation with various stakeholders prior to Governor in Council consideration.

The process for listing entities under the *Criminal Code* involves numerous checks and balances and is based on the necessity that reasonable grounds to believe the entity engages, or engaged, in terrorist activities, and did so knowingly - is met.

There are currently 34 entities listed under the *Criminal Code* (see response 1.9). Twenty-one (21) of those are not listed by the Al Qaida and Taliban Sanctions Committee and include:

Abu Nidal Organization, Aum Shinrikyo, Basque Fatherland and Liberty, Gamma'a al-Islamiyya, Hamas, Hizballah, Kurdistan Worker's Party (PKK), National Liberation Army (ELN), Revolutionary Armed Forces of Colombia (FARC), United Self-Defense Forces of Colombia (AUC), Shining Path (Sendero Luminosa – SL), Palestinian Islamic Jihad (PIJ), Palestinian Liberation Front (PLF), Popular Front for the Liberation of Palestine (PFLP), PFLP-General Command (PFLP-GC), Lashkar E-Tayyiba, Al-Aqsa Martyrs Brigade, Vanguards of Conquest, Babbar Khalsa International, Babbar Khalsa, International Sikh Youth Federation.

A complete listing of those on the *Criminal Code* list can be seen at:
http://www.psepc.gc.ca/national_security/counter-terrorism/AntiTerrorism_e.asp

The process for listing entities under the *Criminal Code* is established in legislation and is driven by threats to the security of Canada. As previously indicated, the process involves numerous checks and balances and is based on the necessity that reasonable grounds to believe the entity engages, or engaged, in terrorist activities, and did so knowingly - is met.

The time-line for listing an entity varies from case-to-case and is dependant upon such factors as the amount and quality of information available, ability to meet the legislative test for listing and decision of the Governor in Council.

To date no persons or entities have been prosecuted for inviting support for proscribed organizations and/or other terrorist groups or organizations under the provisions in the *Criminal Code*.

1.17 Please outline the legal and administrative procedures developed by Canada to protect port facilities, ships, persons, cargo, cargo transport units, off-shore installations and ship's stores from risks of terrorist attacks. Have competent Canadian authorities put appropriate procedures in place to enable them to review and update Canada's transport security plans as and when appropriate?

On January 22, 2003 the Minister of Transport, on behalf of the Government of Canada, announced a five-year package of initiatives of up to $172.5 million designed to further enhance the security of Canada's marine transportation system and maritime borders. The marine security projects focus on safeguarding and protecting our marine infrastructure, surveillance of Canadian waters and improving our emergency response capabilities. Specific projects include: increased surveillance and tracking of marine traffic, including "near real-time" identification and tracking of vessels in Canadian waters; screening of passengers and crew on board vessels; installing new detection equipment in ports to screen containers for radiation; new funding for the enhancement of the RCMP Emergency Response Teams and the establishment of permanent investigator positions at major ports; making further improvements to port security by establishing restricted areas and requiring people working within these areas to undergo thorough background checks; counter-terrorism training exercises; visas for seafarers joining ships in Canada; and developing and implementing new security requirements in line with recent recommendations of the International Maritime Organization (IMO).

http://www.tc.gc.ca/n_ .iaaroom/releases/nat/2003/03-gc001.htm

In order to implement the IMO's International Ship & Port Facility Security (ISPS) Code, which requires SOLAS class ships on international voyages and port facilities that service them, to conduct security assessments and develop security plans, Canada has developed regulations. The draft regulations, expected to be promulgated in Spring of 2004, can be found at:
http://www.tc.gc.ca/vigilance/sep/marine_security/regulatory_menu.htm

As required by the ISPS Code, port facilities determine, in consultation with Transport Canada, when it is necessary to update the security plans and then resubmit them to the Transport Canada for approval. Enforcement and compliance of international environmental and safety standards are handled by the Port State Control.

1.18 Has Canada implemented the standards and recommendations of the International Civil Aviation Organization (Annex 17)? Could Canada inform the CTC when the ICAO safety audit of Canada's international airports has been completed?

Canada is committed to implementing the standards and recommendations of the International Civil Aviation Organisation (ICAO).

Canada implements its Annex 17 obligations through a comprehensive and integrated national program of legislation/regulations, regulatory oversight and enforcement, intelligence, training, awareness and other elements. Authority for the development, maintenance and implementation of Canada's aviation security program is vested with the Minister of Transport under the *Aeronautics*

Act, which gives the Minister responsibility for the development and regulation of aeronautics and the supervision of all matters connected with aeronautics, including aviation security. Day-to-day administration of the program is conducted by Transport Canada. The Canadian Air Transport Security Authority (CATSA), is a Crown corporation based in the National Capital Region and came into existence on April 1, 2002 through Bill C-49. CATSA reports to Parliament through the Minister of Transport and is responsible for security screening operations at Canadian airports.

Further information on Canada's aviation security program - including applicable legislation/regulations - can be found at the following websites:

http://tcinfo/vigilance/en/securityemergencypreparedness/nationaltransport/policy/aviation.htm

http://www.catsa-acsta.gc.ca/english/index.htm

Canada has not yet been audited under ICAO's Universal Security Audit Programme (USAP) and is not scheduled to be audited in 2004.

1.19 The CTC would appreciate it if Canada could provide an outline of the steps which it has taken or which it proposes taking in regard to:

The ratification and implementation of the United Nations Convention against Transnational Organised Crime and the supplementary Protocol against the Illicit Manufacturing of and Trafficking in Firearms, Their Parts and Components and Ammunition:

Canada takes the ratification process very seriously and is working diligently to ensure full and proper compliance. Prior to the ratification of an international legal instrument by Canada, the government must ensure that a domestic regime is in place that will allow the implementation of commitments Canada is about to undertake under the treaty.

Canada has already ratified the Convention and the two other Protocols. The process leading to the ratification of the *Protocol Against the Illicit Manufacturing of and Trafficking in Firearms Their Parts and Components and Ammunition*, supplementing the *United Nations Convention Against Transnational Organized Crime*, requires the drafting and adoption of new legislation and regulations. Both involved going through a lengthy and complex process (detailed below).

The necessary legislative amendments were enacted in May 2003. The legislative process is now complete but the necessary regulations to bring Canada into full conformity with the Protocol are still being developed.

The regulatory process is well underway. Following reviews by the appropriate House of Commons and Senate Committees, the government will consider any Parliamentary recommendations, as well as comments received from the public, with a view to finalizing the regulations.

Once the regulations are in place, a formal decision by the federal Cabinet is then required before Canada can file the necessary instrument of ratification. In the interim, Canada has stringent laws and administrative measures for controlling the import and export of firearms, parts, components and ammunition, and for controlling the possession and transfer of such items while they are in the country.

The implementation of the Recommendations of the World Customs Organisation (WCO) concerning the above mentioned Protocol

The Canada Border Services Agency (CBSA), as a member of the WCO, supports both the Recommendation of the Customs Co-Operation Council on the Insertion in National Statistical Nomenclatures of Subheadings to Facilitate the Monitoring and Control of Products Specified in the Protocol Concerning Firearms Covered by the *UN Convention Against Transnational Organized Crime* and the Recommendation of the Customs Co-Operation Council Concerning the *Protocol Against the Illicit Manufacturing of and Trafficking in Firearms, their Parts and Components and Ammunition*.

The Legislative amendments introduced to help Canada ratify the UN Protocol received Royal Assent in May 2003. The CBSA is awaiting the finalization of the associated regulations and their coming into force in order to fully implement the UN Protocol and the WCO Recommendations.

The use of electronic reporting and the promotion of the security of the supply chain as provided for in the General Annex to the revised WCO Kyoto Convention, as well as the standards of the WCO

Canada supports the revised WCO *Kyoto Convention* and was one of the first signatories. It has not yet been implemented. Canada participated in World Customs Organization Task Force on Security and Facilitation of the International Trade Supply Chain.

Canada was one of the lead countries in the development of the WCO Resolution on Security and Facilitation of the international trade supply chain that included:

- Full review of the WCO Data Model by Summer of 2003;
- - Guidelines to assist members to develop legal basis and necessary processes to enable the advance electronic transmission of customs data;
- Cooperative arrangements between members and industry on the security and facilitation of the international trade supply chain;

Canada was the first country to implement WCO data model and is an active member of the WCO Information Management Sub-Committee as well as the WCO Data Model Working Group.

The implementation of the Programme of Action (adopted by the UN Conference to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons.

This summary pertains to the implementation by Canada of the United Nations (UN) Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons in All Its Aspects (UN Programme of Action). The full report was presented to the (UN) Department of Disarmament Affairs at the Biennial meeting of States to consider the Implementation of the Programme of Action on Small Arms in July 2003 a copy of which is available under UN Document Symbol A/CONF.192/BMS/2003/CRP.48 .

National Level

The Canadian National Committee on Small Arms and Light Weapons is Canada's national coordination body that advises the government on the implementation of the UN Programme of Action, assists in coordinating this implementation and fosters the exchange of information on SALW activities.

The possession, export controls, brokering, marking / tracing / record keeping, disposal and illegal aspects of SALW fall under an assortment of legislations, regulations and administrative procedures. These include the *Firearms Act*, the *Export and Import Permit Act*, the *Defence Production Act*, the Controlled Goods Program, the *United Nations Act*, the Wassenaar Arrangement and the *Criminal Code*. A number of bodies are responsible for various aspects of SALW including the Royal Canadian Mounted Police, Department of Foreign Affairs and International Trade, Department of National Defense, the Criminal Intelligence Services Canada, National Police Services and the Canadian Firearms Centre.

Canada has signed the Protocol against the Illicit Manufacturing of and Trafficking in Firearms, Their Parts and Components and Ammunition, supplementing the United Nations Convention against Transnational Organized Crime and the Inter-American Convention against the Illegal Manufacturing of and Trafficking in Firearms, Ammunition, Explosives and Other Related Materials of the Organization of the American States. Amendments to the *Firearms Act*, tabled in Parliament in March 2001 and passed in May 2003, will pave the way for the drafting of regulations to ensure that Canada is compliant with the firearms provision of both documents.ith the enactment of new legislation, expected in 2004, the entire responsibility for the import of firearms would shift to the Canadian Firearms Centre. Legislation that would permit Canada to require more fulsome marking of newly manufactured or newly imported firearms has received Royal Assent, but enabling regulations are currently under consideration following recommendations from consultations with Parliamentary committees. Finally, in keeping with multilateral commitments, Canada will soon introduce in-transit regulations permitting the transit, through Canada, by businesses, of restricted and non-restricted firearms.

Regional Level

Since 2001, Canada has supported, and continues to support, a variety of workshops and seminars, in Central and South East Asia, Latin America, Africa and Eastern Europe on the implementation of the UN Programme of Action. Furthermore, Canada has provided expertise at several levels to the international community and has contributed to an array of activities, including, but not limited to,

disarmament, training, research and reintegration programmes, in Moldova, Albania, Serbia Montenegro, Latin America and the Horn of Africa and the Great Lakes region.
Canada is an active participant in the Wassenaar Arrangement. Civil society representatives in Canada are also engaged on the issue through the annual government-NGO consultations on peace-building and human security and through the new National Committee on SALW.

Global Level

Canada usually implements sanctions imposed by the United Nations Security Council through regulations made under the *United Nations Act*. Once regulations are in place, Canadian authorities such as the Canada Customs and Revenue Agency are responsible for inspecting and detaining goods that are in violation of the sanctions. The RCMP may be called to investigate and lay charges.

Canada adheres to the reporting requirements of the Wassenaar Arrangement, under which Participating States exchange information on deliveries to non-participating states of conventional arms. Canada submits annual reports to the UN Conventional Arms Register and to the OSCE. In addition, the marking system of the Canadian Armed Forces has been reported to the OSCE. The RCMP National Police Services is in the process of developing a national strategy on firearms smuggling to foster improved sharing of intelligence and operational support and the Department of National Defence conducts a wide range of training in the general fields of physical security of facilities, general inventory control, record management, etc.